様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　６　月　　２　日現在

機関番号：　１２６０１
研究種目：　基盤研究(B)（一般）
研究期間：　2013～2016
課題番号：　２５２８０００１

研究課題名（和文）消失と誤りを含む秘密鍵からの鍵復元に関する研究

研究課題名（英文）Study on Secret Key Recovery from Noisy Versions

研究代表者
　國廣　昇（Kunihiro, Noboru）

　東京大学・新領域創成科学研究科・准教授

　研究者番号：６０３４５４３６

交付決定額（研究期間全体）：（直接経費）　　5,900,000円

研究成果の概要（和文）：本研究課題では，ノイズ付きの秘密鍵が得られたときに，秘密鍵全体を復元するアルゴリズムの提案を行った．正しい秘密鍵に対して，消失と誤りが生じた状況に対して研究を行い，理論限界を達成するアルゴリズムを提案した．さらに，物理的な観測によりアナログの値が得られる状状況の研究を行った．観測値が従う確率分布の知識に応じて，4つのアルゴリズムを提案した．さらに，EMアルゴリズムと組み合わせることにより，事前の知識が不要でありながら，効率的なアルゴリズムの提案を行った．いずれも，数値実験を行い，提案アルゴリズムの有効性を確認した．

研究成果の概要（英文）：In this research project, we proposed several algorithms to recover the whole secret key when secret key sequences with noise are obtained. We studied the situation where the erasure and error occurred to the correct secret key and proposed an algorithm to achieve the theoretical bound. Furthermore, we conducted a study on the situation that analog values can be obtained by physical observation. We proposed four algorithms according to the knowledge of the probability distribution followed by observed values. We then proposed an efficient algorithm without prior knowledge by combining with the EM algorithm. In both cases, we conducted numerical experiments and confirmed the effectiveness of the proposed algorithms.

研究分野：　暗号理論

キーワード：　暗号理論　安全性評価　サイドチャネル攻撃

１．研究開始当初の背景

(1) 研究の社会的背景

暗号技術の広がりとともに，IC カードや RFID などの物理的なデバイスに暗号技術が搭載されるようになっている．暗号技術を使う上で，秘密鍵は，デバイスに安全に保持される必要があり，通常，耐タンパー技術のような物理的な技術により，鍵が守られている．理想的には，これらの秘密鍵に代表される秘密情報は，厳重に管理されているはずであるが，現実の運用を考えた場合には，秘密情報が部分的に漏洩してしまうことを考慮する必要がある．例えば，IC カードなどの，それほど高価ではなく，厳重な漏洩対策がされていないデバイスから，電力，電磁波などを観測することにより，秘密鍵の情報が漏れる攻撃が考えられている．これらの外部的な脅威に対しても，安全である暗号システムが社会的に求められている．

(2) 研究の学術的背景

物理的なデバイスに格納された秘密情報を，外部から何らかの物理量を測定することにより，あばく攻撃は総称して，サイドチャネル攻撃と呼ばれている．サイドチャネル攻撃にさらされている環境下では，鍵の全てが推測されてしまうわけではなく，ほとんどの場合，ノイズなどにより汚れた秘密鍵が入手できると想定される．それ以外の状況として，仕様の稚拙や悪い実装により，不意に秘密情報が漏れることもある．鍵の全てが推測できるわけではなく，一部しか推測できない場合は，必ずしも，直ちに脆弱性が生じるとは限らない．しかし，どこまで漏洩した場合には，危険であるのかの見極めは，一般に困難である．当然，全ての秘密情報が漏れた場合は，安全にはなり得ないが，少量の秘密情報が漏れた場合では，依然，安全性は保たれる．それでは，どの程度，情報が漏れれば，危険になるのであろうか？どの程度情報がもれると安全でなくなるかの見極めは，ハードウェアの設計においてきわめて重要である．この見極めにより，コストを重視して，ある程度の秘密情報の漏洩は妥協しながらも，安全性を確保したまま，コストを抑えたハードウェアの設計が可能となる．

当然，秘密鍵の「全て」が入手できる状況であるならば，攻撃者と正規の受信者の間に能力差は生じないので，このような状況では，いかなる安全な方式を構成することも不可能である．多くの現実的な攻撃環境では，攻撃者は秘密鍵の「断片」を誤りを含んだ形で入手することになる．

暗号の安全性評価を机上ではなく，実際の暗号化を行うデバイスに対する評価を行った最初の研究は，1996 年に提案された Kocher による電力差分攻撃である．これは，暗号化を行う装置の使用電力を計測し，その使用電力を統計的に処理を行い，そのデバイスに埋め込まれた秘密鍵を復元する攻撃である．この方法において漏れだす情報は，消費電力であり，消費電力と実際の鍵の値には強い相関があるため，電力を計測することにより，鍵の復元が可能となる．消費電力は，当然，多くのノイズが乗った状況で観測されるため，汚れた情報から，正しい鍵を推測するためには，統計処理等の技術が必要となる．その後，電力だけでなく，漏洩する電磁波を用いた攻撃や，複数箇所の電力を計測することにより，より少ない計測回数で鍵を算出する攻撃も提案されている．

本研究課題では，もう少し具体的な値，すなわち，消失または誤りにより，汚れた秘密鍵が入手できた状況下で，きれいな秘密鍵を復元する攻撃を考える．これまでに，2008 年の Helderman らの攻撃，2009 年の Heninger らの攻撃，2010 年の Henecka らの攻撃などが提案されている．しかしながら，これまでの研究では，

- いずれの提案アルゴリズムも，ad-hoc なアルゴリズムであり，最適性などが確認されていない，
- 誤りのクラスが限定されているため，それ以外の複雑な誤りが生じた場合には対処ができない，

などの問題点があった．

２．研究の目的

本研究の目的は，ノイズなどにより「汚れた」秘密鍵から，効率的に正しい秘密鍵を復元するアルゴリズムの提案である．すなわち，公開鍵暗号，共通鍵暗号において，部分的に値が消失する，もしくは，誤りを含む，または物理的な観測により連続量として，秘密鍵が得られたときの安全性評価を詳細に行うことを主たる目的とする．IC カードのような安価で，ある程度の漏洩を許容せざるを得ない状況では，漏洩する量と製造コストは密接な関係がある．どの程度漏洩してしまうと，安全性が損なわれるかを厳密に調べることにより，どの程度のコストをかけて製品の製造を行えばよいかの評価を行うことが可能となる．これにより，物理的な攻撃にさらされた環境下でも安全に暗号を用いることが可能となり，適切なコストにより，暗号システムの運用が可能となる．

本研究では，ad-hoc の研究からの脱却を試み，より高い見地に立ち，最適なアルゴリズムの探索を目指す．効率的で，広い誤りのクラスに対しても適応できるアルゴリズムの探索だけでなく，理論限界に関する研究も行う．理論限界を知ることにより，ここまで効率化を行ったとしても，脆弱性に結びつかないという極限までの設定を行うことが可能となる．

３．研究の方法

(1)　本研究課題の目的は，ノイズが乗った秘密鍵から，正しい秘密鍵を復元するアルゴリズムに関する研究を行う．その際の主たる道具として，誤り訂正符号や格子理論に関する知見を利用することにより，効率的なアルゴリズムの探求を行う．アルゴリズムの探求にとどまらず，攻撃の理論限界を見極めることが重要である．また，既存の研究では，現実の物理的な鍵漏洩と，モデルの間には大きな乖離があったが，現実的な物理モデルの下で漏洩が行われた時に，安全性を保持できる方式の提案を行う予定である．さらに，数値実験により，提案手法の有効性を確認し，理論的な限界の妥当性を検証する．

(2)　本研究の遂行において，秘密鍵に関する何らかの情報が漏洩されたときに，いかにして，そこから秘密鍵を復元するかが重要な点である．逆に，どの程度情報を漏洩から守ることが出来れば，秘密鍵の復元を阻止できるかを考えることにもなる．これは，どこまでコストを抑えたとしても，安全性は担保することができるのかを考えることに相当する．実際，RSA 暗号における秘密情報である p は奇素数である．そのため，最下位ビットは 1 であるということは，既知であり，漏洩情報とみなすことができるが，もちろん，この情報だけから，素因数分解を行うことは不可能である．どの程度の情報がわかれば，秘密鍵のすべてがわかるかという問題は，解決が自明な問題ではない．次に，サイドチャネル攻撃のように，誤りが乗った秘密鍵が得られる状況も想定する．この状況でも，誤りを訂正し，正しい鍵を復元する問題は，必ずしも自明ではない．さらに，現実の状況では，消失と誤りが複合的に生じると考えなくてはならない．さらに，離散的な情報ではなく，物理的な観測値として，連続量が得られるという状況の方が自然である．RSA 暗号において，秘密鍵は冗長性を含んでおり，全ての秘密情報が復号処理において必要ではない．しかし，その冗長性をうまく利用することにより，復号のスピードをあげることが可能である．その一方で，この冗長性を利用することにより，秘密鍵が，消失や誤り，物理的な観測により「汚れて」しまっても，もとの綺麗な誤りのない秘密鍵を復元することが可能となる．

(3)　これまでの研究では，ad-hoc なアルゴリズムの提案にとどまっていたが，系統的な解析を試みる．解析のアプローチとして，情報論的なアプローチ，格子理論によるアプローチの二方向を選択する．

　前者のアプローチ（情報論的なアプローチ）においては，以下の戦略を取る．消失がある，誤りを含む，もしくは物理的な観測によりノイズが乗った秘密鍵から正しい秘密鍵の全てを復元する問題とノイズがある通信路を通した符号語から，もとの情報を復元する問題の類似性に着目する．誤り訂正符号に関しては，古くから研究がなされており，多くの知見（効率的なアルゴリズム，理論的限界など）が得られている．その一方で，計算機環境の進展を契機に，古いアルゴリズムの再発見，新たな効率的なアルゴリズムの開発などが行われ，依然，活発に研究が行われている．本研究では，これらの最先端の研究の成果を積極的に活用することにより，性能の良いアルゴリズムの提案を試みる．しかしながら，ターゲットとする問題（ノイズの乗った秘密鍵から正しい秘密鍵を復元する問題）と誤り訂正符号では，完全には問題が対応していないため，適切な問題の読み替えが必要となる．この適用を，できるだけ，システマテッィクに行い，どのようなタイプのノイズに対しても，対応させることが本研究のポイントである．

　後者のアプローチ（格子理論によるアプローチ）に関しては，以下の戦略を取る．秘密鍵の部分情報が得られた状況を代数方程式で記述し，その方程式を解くことにより，秘密鍵全体を復元するアプローチである．代数方程式を解くアルゴリズムに関しては，様々な問題に対して，多くの研究がなされている．これらの知見を用いることにより，ターゲットする問題に対する効率的なアルゴリズムの探索を目指す．

　前述したように，これまでの研究には，以下のような問題点があった．

1. いずれの提案アルゴリズムも，ad-hoc なアルゴリズムであり，最適性などが確認されていない
2. 誤りのクラスが限定されているため，それ以外の複雑な誤りが生じた場合には対処ができない

1.の問題点に関しては，何らかの意味での最適性が言えない限り，安心して暗号を用いることが困難となる．一般的に，既知の攻撃に対して安全性が担保されるように暗号を設計した場合，新たな強力な攻撃が発見された場合には，システム全体の崩壊を招くことになる．その一方で，あまりにも安全サイドに倒し，マージンを取りすぎると，著しく効率を劣化させることとなる．そのため，適切なパラメタ設定が必須となるが，そのためには，最適性の議論が必ず必要となる．そのため，理論限界の探求と適用範囲の広いアルゴリズムの両方の研究が必須となる．2.の問題点に関しては，物理現象である限り，複雑な誤りのパターンが生じる可能性がある．デバイスにより，誤りのパターンが異なることもありうる．また，安全性向上等の為に，意図的に誤りをのせる場合には，設計者が意図的に，複雑な誤りを乗せることが可能である．

４．研究成果

(1) ノイズ付き秘密鍵が得られたときの RSA 暗号の安全性解析

秘密鍵の各ビットの値に応じたアナログ値が観測される状況に焦点をおいて研究を行った．この漏洩モデルにおいては，正しいビット自身が観測できるのではなく，正しいビットにある種のノイズが乗った値が観測される．従来の研究では，デジタルの値が観測される場合の解析しか行われてこなかった．しかし，実際に，サイドチャネル攻撃の状況を考えると，デジタルの値が直接得られるわけではなく，最初の段階では，アナログの値が観測されると考えた方が自然である．

平成 25 年度には，このノイズモデルに対して，秘密鍵を完全に復元する 2 種類のアルゴリズムを提案し，それぞれの提案アルゴリズムにより，多項式時間で復元できるためのノイズの条件を明らかにした．一つ目のアルゴリズムは，ノイズの分布が正確にわかっている場合のみに有効なアルゴリズムである．二つ目のアルゴリズムは，ノイズの分布がわからない場合にも有効なアルゴリズムである．提案アルゴリズムでは，鍵の候補系列を，ある基準に従い，残す／捨てる，の判定を行い，最終的に，正しい鍵が残る仕組みを採用している．ここで，重要になるのは，この基準をいかに設定するかである．提案アルゴルズム１では，尤度，正確には，対数尤度の比を，その基準に設定している．そのため，このアルゴリズムでは，ノイズ分布を正確に知る必要がある．提案アルゴリズム２では，電力差分攻撃で用いる関数を参考にした基準を設定している．この基準は，純粋に，候補系列と観測値のみから計算されるため，分布を知らなくても計算可能である．秘密鍵の復元に成功するための条件に関しては，連続確率密度関数に対する微分エントロピーを用いることにより，厳密な評価を与えている．この評価により，一つ目のアルゴリズムの方が，より大きいノイズに対しても，秘密鍵の復元が可能であることを示した．さらに，ノイズがガウス分布に従うときには，二つ目のアルゴリズムは，一つ目のアルゴリズムと同等の性能を持つことを示した．また，数値実験により，提案アルゴリズムの有効性を示した．

平成 28 年度には，この安全性評価の拡張を行った．従来提案されているアルゴリズムでは，ノイズに関する統計情報が完全にわかっているとき，および，何もわからないときという，理想的な環境のみに適用可能であった．また，従来のアルゴリズムでは，対称のノイズに対して，特に有効であったが，非対称なノイズに対しては，必ずしも，有効ではなく，改良の可能性が示唆されていた．本研究では，従来の攻撃手法を拡張し，推定分布がわかっている時，およびノイズの分散がわかっている時に有効なアルゴリズムの提案を行い，攻撃の成功条件を求めた．まず，推定分布がわかっているときに有効なアルゴリズムの提案を行い，厳密な攻撃の成功条件の導出に成功した．推定分布と正しい分布とのある種の距離が大きくなればなるほど，攻撃成功条件は悪くなる．逆に言えば，正しく推定できればできるほど，攻撃に成功しやすいことを示している．さらに，各分布の分散値が既知であるときに，分散値をスコア関数に陽に組み込むことに成功し，大きいノイズに対しても，鍵の復元が可能な手法を提案した．さらに，攻撃の成功条件を示した．しかし，このアルゴリズムは，分散値を陽に用いているため，この値を知らない状況では機能しない．この問題を克服するために，学習理論でよく用いられる EM アルゴリズムを利用するアルゴリズムを提案した．まず，観測系列から，分散値を推定し，その推定した分散値を利用し，前述のアルゴリズムを用いることにより，観測データからの攻撃に成功している．数値実験を行い，従来のアルゴリズムよりも，高い確率で攻撃に成功することを確認した．

RSA 暗号の離散的なノイズ付き秘密鍵からの鍵復号において，鍵の復元に成功する際に満たすべき消失確率と誤り確率の関係の理論限界は知られていたが，その限界を達成するアルゴリズムは知られていなかった．平成 27 年度には，アルゴルズムのフレームワークは変更せずに，評価をより厳密に行うことにより，理論限界を達成することに成功した．さらに，この考えを応用し，ストレージに秘密鍵を保存する際に，あえて，ノイズを乗せることにより，サイドチャネル攻撃に耐性のある手法を提案した．

(2) ノイズ付きの key scheduling が得られたときの共通鍵暗号の安全性解析

攻撃の対象を，公開鍵暗号だけでなく，共通鍵暗号の AES，SIMON にも広げ，安全性解析を行った．AES は，現在，非常に広く使われている暗号方式であり，SIMON は，NSA により提案された共通鍵暗号方式であり，その安全性解析は極めて重要である．鍵サイズが 128 ビット AES に対して，消失はなく，誤りが生じた場合の安全性解析を行った．鍵スケジュールの各ビットが，確率 p でビット反転するときに，どの程度の大きい p に対して，秘密鍵の復元が可能であるかを検証した．その結果，理論的には，$p<0.324$ の時，鍵復元が可能であることを示した．さらに，数値実験を行い，$p<0.20$ のときには，攻撃に成功することを明らかにした．共通鍵暗号 SIMON に対しても，ノイズ付きの key scheduling が得られた時に鍵復号アルゴリズムの提案も行った．

(3) 格子理論を用いた RSA 暗号およびその変種方式に関する安全性解析

RSA 暗号において，秘密鍵の上位ビット，下位ビットが漏洩したときの安全性評価を行った．従来のアルゴリズムよりも，より広いクラスに対して，攻撃に成功するアルゴリズ

ムの提案に成功している．漏洩情報が，小さい時の挙動は，漏洩情報がない場合と同じ挙動を示すことが期待されるが，従来のアルゴリズムは，これを実現していないという問題点があった．まず，漏洩情報量を 0 に近づけた場合に，漏洩情報がない場合に特化したアルゴリズムと同じ限界を達成するアルゴリズムを提案した．この結果により，漏洩情報が少ない場合に，従来のアルゴリズムよりも，大きい秘密鍵に対して，攻撃に成功する．

この種の攻撃は，様々な攻撃シナリオにおいて多くの研究がなされているが，本研究では，その一般化を行い，従来の研究を包含するとともに，従来よりも，強力な攻撃の提案に成功している．単なる一般化だけではなく，安全性評価をする際に，ツールキットとして利用することが可能である．さらに，３つ以上の素数の積からなる公開鍵を用いる RSA 暗号の変種方式に対する安全性解析も行った．秘密鍵の下位ビットが漏洩したときの安全性評価を行い，従来の方式よりも強力な攻撃の提案に成功している．

中国人の剰余定理を用いた高速化を行った RSA 暗号に対して，秘密鍵の部分情報が得られた時に，鍵の復元が容易になることが知られている．本研究では，公開鍵 e の値が，n と同程度のときにも，有効な攻撃の提案を示している．さらに，評価対象を広げ，p の r 乗×q タイプの RSA 暗号に関しても，秘密鍵の部分情報が漏洩した時の安全性および秘密鍵が小さい時の安全性に関して解析を行った．

(4) 格子暗号の安全性評価

格子暗号の安全性の根拠となる LPN 問題, LWE 問題，最短ベクトル探索問題に対して解析を行い，従来よりも優れたアルゴリズムの提案に成功した．LPN 問題，LWE 問題に関して，ノイズが小さい時の安全性に関して解析を行い，従来の想定よりも，脆弱であることを明らかにした．さらに，最短ベクトル探索問題に対しても，従来の方式の拡張を行うことにより，より少ないメモリ量で同等の計算時間で解を出力するアルゴリズムの提案を行った．

５．主な発表論文等

〔雑誌論文〕（計 24 件）

1. Improved Key Recovery Algorithms from Noisy RSA Secret Keys with Analog Noise, N. Kunihiro and Y. Takayasu, in Proc. of CT-RSA2017, LNCS10159, pp.328-343, 2017.
2. An Improved Attack for Recovering Noisy RSA Secret Keys and its Countermeasure, N. Kunihiro, in Proc. of ProvSec2015, LNCS 9451, pp. 61-81, 2015.
3. サイドチャネル攻撃の数理 (特集 暗号と数学), 國廣昇, 数学セミナー 2015 年 7 月号, pp. 34-39, 2015.
4. RSA meets DPA: Recovering RSA Secret Keys from Noisy, N. Kunihiro and J. Honda, in Proc. of CHES2014, LNCS 8731, pp. 261-278, 2014.
5. Recovering RSA Secret Keys from Noisy Key Bits with Erasures and Errors, N. Kunihiro, N. Shinohara and T. Izu, IEICE Transactions, Vol. E97-A, No.6, pp. 1273--1284, 2014.

〔学会発表〕（計 20 件）

1. Recovering RSA Secret Keys from Noisy Keys, N. Kunihiro, UTokyo-IIT Madras Workshop on Theoretical Computer Science, Chennai, India, 2017 年 3 月 14 日.

６．研究組織

(1)研究代表者

國廣　昇　（KUNIHIRO, Noboru）
東京大学・大学院新領域創成科学研究科・准教授
研究者番号：60345436